



UNIVERSITY POLICY

SUBJECT:	INFORMATION SERVICES AND TECHNOLOGY	TITLE:	ACCESS TO UNIVERSITY-ADMINISTERED SOFTWARE SYSTEMS		
CATEGORY: Check One	Board of Trustees <input type="checkbox"/>	Presidential <input checked="" type="checkbox"/>	Functional <input type="checkbox"/>	School/Unit <input type="checkbox"/>	
Responsible Executive:	Vice President for Information Services and Technology		Responsible Office:	Information Services and Technology	
CODING:	00-01-95-10:00	ADOPTED:	04/22/02	AMENDED:	03/17/10
			LAST REVIEWED: 03/17/10		

I. PURPOSE

To establish the principles and set the overall University policy framework by which access to University-owned, leased or licensed software systems, databases and networks are controlled and protected.

II. ACCOUNTABILITY

Under the President, the Executive Vice President and Senior Vice Presidents shall ensure compliance with this policy. The Vice President for Information Systems and Technology (IST), the Presidents/CEOs of the Healthcare Units, Deans and Vice Presidents shall implement this policy by means of Unit- and system-specific procedures, guidelines and standards.

III. DEFINITION

- A. Institutional Data and Information - all information collected, built, created, discovered, generated, stored, purchased or leased by the University or its employees, students and agents, to support the University’s research, teaching, service and patient care missions and its financial and administrative activities, regardless of the medium, form or location.
- B. Electronic Information Resources - all computing machinery, networks and communication equipment and networks.
- C. System Administrator - the designated person responsible for setting up and maintaining hardware and/or software.
- D. Data Steward (also called Data Custodian) - the person designated by the pertinent President(s)/CEO(s) of the Healthcare Units, Dean(s) or Vice President(s) to be responsible for the management of particular datasets, as vested by University personnel, offices, Schools or Units responsible for the creation or collection of the data.

IV. REFERENCES

- A. Information Management [00-01-10-30:00](#)
- B. Rights & Responsibilities for the Use of University-Accessed Electronic Information Systems [00-01-10-40:00](#)

- C. Family Educational Rights and Privacy Act [00-01-25-05:00](#)
- D. Patient Confidentiality and Health Information [00-01-40-60:00](#)

V. POLICY

A. General Principles

1. The University owns its computing, networking, telephony, video and other communications systems and its information resources and has the right to monitor them. The University also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The University has the responsibility for the security, integrity, maintenance and confidentiality of the electronic systems.
2. Computing, networking, telephony, video and information resources of the University, including access to local, national and international networks, exist to support students, faculty and staff as they carry out the education, research, healthcare and public service missions of the University. Toward these ends, the University encourages and promotes the use of these resources by the University community.
3. As part of the planning for new computing, networking, telephony and/or information resources in any UMDNJ School/Unit, a written communication to the Vice President of Information Systems and Technology will be initiated by the Department Head or designee in order to ensure adherence to the general policy and to plan for allocation of resources required for technical support.
4. Acknowledging that security access concerns may vary from system to system, Data Stewards and System Administrators shall develop within the specific written procedures for their systems, guidelines to govern the authorization of access to users. These guidelines, consistent with this policy, will encompass access for employees, students and non-employees of the University. The Vice President for Information Services and Technology shall ensure that such policies are established and render assistance to those individuals responsible for their development.
5. Data Stewards and System Administrators shall develop and distribute specific written procedures to protect the rights of legitimate authorized users, to protect the integrity of the information and systems under their management and to delineate the responsibilities of users. The University has the authority to control or refuse access to anyone who violates these procedures or threatens the rights of other users or the availability and integrity of the systems and the information. Actions that may be taken under this authority include deactivating accounts, access codes or security clearances; halting unauthorized or disruptive processes; deleting unauthorized or inappropriate files; and disabling access to computing, networking, telephony and other information resources.
6. Data Stewards shall report suspected security breaches, unauthorized access, audit trail data or other system warnings about unusual or inappropriate activity, violations of policy and weaknesses in security measures within 24 hours of becoming aware of the incident. The report shall be sent to the Vice President for IST who shall initiate an investigation and issue recommendations as appropriate to the President/CEO of the Healthcare Unit, Dean or Vice President of the Unit from which the incident occurred. If warranted, the pertinent President/CEO of the Healthcare Unit, Dean or Vice President will cooperate with the Vice President for IST in the determination of the penalty or sanction to be imposed under this policy.
7. When demand for computing, networking, telephony and other information resources exceeds available capacity or resources, priorities shall be established for allocating the resources, with a higher priority to activities essential to the missions of the University. The Vice President for IST, in consultation with the Presidents/CEOs of the Healthcare Units, Deans and Vice Presidents shall set these priorities.

8. Users shall be trained in the basic principles of this policy as it relates to access, security and confidentiality. In addition, departments will train users concerning specific procedures/guidelines.
9. A registry of contact information will be maintained and published by Information Services and Technology for the purpose of identifying System Administrators and Data Stewards who shall be responsible for implementing this policy in a manner appropriate to their environment.

B. Access

1. Access to institutional databases, servers and networks is a privilege granted by the University, to be used only for those purposes for which the access is authorized. The nature and extent of authorized access to institutional databases, servers and networks shall be determined by:
 - a. legitimate needs to fulfill job responsibilities;
 - b. local/state/federal/funding agency requirements;
 - c. confidentiality requirements; and
 - d. state and federal laws.

Access to and use of these resources for purposes or activities which do not support the University's missions are subject to regulation and restriction to ensure that they do not interfere with legitimate work; and any access to or use of these resources and services that interferes with the University's missions and goals is prohibited. The use and/or release of University data is further restricted under specific laws such as Family Educational Rights and Privacy Act (FERPA) and Health Information Portability and Accountability Act (HIPAA) and laws that govern intellectual property rights.

2. In general, only employees of the University shall have access to confidential information. Under certain circumstances non-employees may be granted access under carefully monitored and restricted conditions. Such access is at the discretion of the Data Steward and/or System Administrator. The access must be justified to have benefit to the operation of the institution. The University will require an executed confidentiality agreement before such access is granted.
3. Privileged access (often called root access) to operating system or database administration tools and interfaces for enterprise systems or systems housing confidential data or information will be at the discretion of the Vice President for IST.
4. Each individual who develops or is given access to institutional databases or networks shall read and understand this policy and all derivative policies, Data Stewards shall report suspected security breaches, unauthorized access, audit trail data or other system warnings about unusual or inappropriate activity, violations of policy and weaknesses in security measures within 24 hours of becoming aware of the incident. The report shall be sent to the Vice President for IST who shall initiate an investigation and issue recommendations as appropriate to the President/CEO, Dean or Vice President of the Unit from which the incident occurred. If warranted, the pertinent President/CEO of the Healthcare Unit, Dean or Vice President will cooperate with the Vice President for IST in the determination of the penalty or sanction to be imposed under this policy.
5. Each individual with access to institutional databases or networks is responsible for all actions and transactions occurring during each exercise of his or her access privilege.
6. Each Data Steward shall have responsibility for:
 - a. approving access to the databases originating in her or his school or unit;

- b. publishing and disseminating the policies and procedures regarding access;
 - c. ensuring prompt (within 24 hours of notification) termination of access for routine changes in an individual's status, e.g., voluntary termination of employment, graduation or withdrawal from the University, or when special vendor or courtesy accounts are no longer needed;
 - d. removing accounts that are inactive or no longer needed; and
 - e. ensuring security compliance for School or Unit level systems.
7. In instances where access is provided to a system and the applications residing therein rather than to a particular database, the management of such systems will be responsible for:
- a. regulating system access to authorized individuals;
 - b. ensuring separation and protection of the data assets of authorized individuals;
 - c. protecting system management applications and attendant data from access by the general usership;
 - d. publishing and disseminating the policies and procedures regarding access;
 - e. ensuring prompt (within 24 hours) termination of access for routine changes in an individual's status, e.g., voluntary termination of employment, graduation or withdrawal from the University, or when special vendor or courtesy accounts are no longer needed
 - f. removing accounts that are inactive or no longer needed; and
 - g. providing security for School or Unit level systems.
8. The Vice President for IST shall be responsible for providing University-wide infrastructure with the proper level of security and authentication mechanisms by which access will be restricted to specific systems, applications and data for authorized users.

C. Confidentiality

1. The categories of institutional information that shall be considered confidential and/or private include, but are not limited to:
- patient healthcare and human subjects research records
 - quality-assurance and peer-review information from patient care units
 - National Practitioner Data Bank information
 - Employee Assistance Program records
 - employees' job performance information
 - student financial aid status, academic and financial records
 - student examination questions
 - private information about students, employees and patients
 - University proprietary information, including copyrightable and patentable information
 - proprietary information belonging to other individuals or entities, such as under a non-disclosure agreement or contract
 - attorney-client privileged information and certain other legal matters
 - library circulation records and any information about use of any library information resource in any format
 - certain business records such as business plans containing competitive information; management memos discussing proposed policies; audit information; contract negotiation strategies; proposed employee wage/benefit information

- executive session minutes from the Board of Trustees and other committees which are not deemed public
- medical and personal information in research records
- records of application for admission to academic programs
- medical and other information pertaining to disability accommodations made to employees and students.

2. Each President/CEO of the Healthcare Unit, Dean and Vice President in conjunction with their Data Stewards, shall develop, publicize and enforce a Unit specific version of this policy, consistent with the provisions herein, and, for the data under his/her authority will:

- a. identify the specific information considered confidential;
- b. define internal role-based need to know and access for each type of confidential information;
- c. define appropriate conditions and procedures for information release, the people authorized to make releases and to receive information;
- d. implement and enforce the standards developed by IST under which confidential information extracted in whole or part from institutional databases may be stored on the internal or removable media of local workstations;
- e. establish retention rules consistent with existing federal, state and local guidelines;
- f. set sanctions for breaches of policy;
- g. assist the Offices of Business Conduct and IST in the promulgation of this policy with regard to general community awareness and orientation/training for individuals with access to confidential and/or sensitive electronic information governed by University or state/federal laws, rules or regulations; and
- h. oversee all vendors, contractors, subcontractors, consultants and external auditors whose scope of work requires access to confidential databases.

D. Security

1. The security of data involves the protection of user files and system and network resources from intentional or unintentional loss, damage, inappropriate access and unauthorized disclosure or use of confidential or private information. Integrity of data is assurance that, once entered, data will not be subject to unauthorized modification intentionally or unintentionally, and that data will remain unaltered during transmission and unintelligible if intercepted between sending and receiving systems. Accountability establishes responsibility for security breaches and audit trails provide the necessary data to explain a security event and provide linkage to the originator. Issues regarding the balance of security against ease of access by authorized individuals will be arbitrated by the Vice President for IST. Security systems techniques include:

- a. authentication of network users and systems, and determination of access and authorization levels (e.g., via passwords, personal identification numbers, digital signatures, token cards, smart cards, one-time passwords, biometrics);
- b. transmission and communications security, protection of remote access points and of external electronic communications (e.g., via firewalls, encryption);
- c. physical security of key network components;
- d. online monitoring, logging and audit trails to maintain information about network access and transactions (e.g., logon activity logs, reference monitors, access alerts);

- e. data integrity technologies (e.g., automated error checking, purge criteria, checksums, system backups, archives, redundant systems, anti-virus software, data disposal schedules);
 - f. ongoing system security assessment (e.g., intrusion monitoring and detection).
2. Each President/CEO of the Healthcare Unit, Dean and Vice President under whom the Data Custodian serves shall be responsible for the security for the databases under his/her authority and for taking disciplinary action for security breaches.
 3. The Vice President for IST shall be responsible for recommending and coordinating University-wide security policies and procedures.
 4. Each Data Steward shall be responsible for implementing and enforcing the security policies and procedures recommended.

VI. NON-COMPLIANCE AND SANCTIONS

The failure to comply with any applicable access and confidentiality policies may result in denial or removal of access privileges to the University's electronic systems; disciplinary action under applicable University policies and procedures; civil litigation; and/or civil or criminal prosecution under applicable state and federal statutes.

By Direction of the President:

Vice President for Information Services and Technology